СПЕКТРАЛЬНЫЕ И КОМБИНАТОРНЫЕ СВОЙСТВА РЕДУЦИРОВАННЫХ ГРАФОВ ДЕ БРЕЙНА

Максимовский А.Ю.[1], Мельников С.Ю.[2]

В статье предложен класс обобщенных графов де Брейна, для которого вычислены спектры и ряд комбинаторных характеристик, включая их диаметр, число петель и циклов длины 2, а также число остовных деревьев, эйлеровых и гамильтоновых циклов. Установлено, что рассматриваемый класс графов замкнут относительно операции построения реберного графа. Указанные свойства указывают на целесообразность применения таких графов при проектировании подсистем контроля защищенности информационных систем, количество элементов которых является составным числом. Это обусловлено тем, что для подсистем контроля, использующих архитектуру графа, обладающего установленными свойствами, можно обеспечить эффективный доступ ко всем элементам системы в целом, ее масштабируемость, гибкую настройку маршрутов обхода элементов с минимальным риском зацикливания. При исследовании влияния числовых параметров рассматриваемых графов на их свойства установлено, что свойство единственности пути заданной длины сохраняется только для «обычных» графов де Брейна. Для получения указанных результатов разработан новый способ вычисления характеристического многочлена k-циркулянтной матрицы в терминах элементов ее первой строки. Это позволило также уточнить ряд известных результатов и упростить процедуры вычисления характеристического многочлена указанных матриц.

Ключевые слова: *регистр сдвига, граф де Брейна, k-циркулянт, спектр матрицы*

DOI: 10.21681/2311-3456-2018-4-70-76

Введение

Граф де Брейна [1, 2] обладает рядом уникальных свойств, которые более ста лет привлекают внимание математиков и инженеров. Значительное число работ посвящено использованию таких графов для задания топологии взаимодействий объектов различной природы. Де Брейновская архитектура конкурентна при построении распределенных вычислительных сетей с архитектурой гиперкуба [3], она эффективна при организации связей между ядрами в мультиядерных процессорах на кристалле [4]. Пиринговые сети, построенные на основе де Брейновской топологии, по целому ряду важнейших характеристик близки к оптимальным [5]. Аппарат графов де Брейна используется для восстановления генома по его фрагментам [6]. Защита информации как в части теории и практики кодирования [7], так и криптографии [8], [9] является одной из основных областей применения таких графов и тесно связанных с ними регистров сдвига.

В литературе предлагались несколько вариантов обобщений графов де Брейна, исходя из условий прикладной задачи. Одним из таких условий является свойство k циркулянтности матрицы смежности графа. Такие обобщения графов де Брейна изучались, в том чиле, в работах [10 - 15] и ряде других. Отметим, что Imase и Itoh в своей оригинальной работе [10] не стремились обобщить графы де Брейна, но искали графы с минимальным диаметром (для оптимизации сетевой архитектуры микропроцессоров), в тексте их статьи графы де Брейна не упоминаются.

Другое направление обобщения графов де Брейна, представленное, в частности, в работах [16], [17] и др., основано на сохранении свойства единственности пути фиксированной длины между любыми двумя вершинами графа. Оба направления обобщений графа де Брейна тесно связаны между собой. Обзор литературы по данной проблематике представлен в [18], см. также [19].

Рассматриваемые в данной статье графы образуют подкласс обобщенных графов де Брейна в смысле [10] и [11]. Однако рассматриваемый случай соответствует наиболее содержательной в комбинаторном смысле ситуации, когда количество вершин графа кратно степени его регулярности. Такие графы в семействе всех обобщенных графов де Брейна являются в определенном смысле «самыми близкими» к классическим графам де Брейна. Визучается статье вид характеристического многочлена матрицы смежности рассматриваемых графов. Спектры одного из классов обобщенных графов де Брейна изучались в [19], однако результат, представленный в данной статье, является независимым и опирается на метод нахождения спектра, не публиковавшийся ранее.

Отметим, что ранее характеристики редуцированных графов де Брейна мало изучались как в целом, так и в целях оптимизации контроля защищенности информационных систем, количество элементов которых является составным числом. В [20] рассмотрен вопрос о планарности таких графов, в [21] получено выражение для числа регистров сдвига, ассоциированных с такими графами и устанавливаемых постоянным входом в фиксированное состояние. Групповые свойства подстановок, реализуемых указанными регистрами сдвига, изучались в [22].

1 Максимовский Александр Юрьевич, кандидат физико-математических наук, старший научный сотрудник ФГБУН Институт проблем управления им. В.А. Трапезникова РАН, г. Москва, Россия. E-mail: maximay@ipu.ru

2 Мельников Сергей Юрьевич, кандидат физико-математических наук, старший научный сотрудник ООО «Лингвистические и информационные технологии», г. Москва, Россия. E-mail: melnikov@linfotech.ru

Редуцированным графом G(n,m) де Брейна назовем граф на множестве вершин , в котором из вершины $(in+\varepsilon)(\operatorname{mod} nm)$, $\varepsilon\in\Omega_n$, выходит ровно *n* дуг, заходящих в вершины $(in+\varepsilon)(\operatorname{mod} nm)$, $\varepsilon\in\Omega_n$ *n=1,2,..., m=1,2,....*

Матрица $A(G(n,m))$ смежности такого графа состоит из n раз повторенных участков по *m* строк в каждом. В каждой строке имеется ровно *n* единиц. Отметим, что матрица $A(G(n,m))$ представима в виде тензорного произведения

$$A(G(n,m))=(1\ \ 1\ \ \cdots\ \ 1)^T\otimes E\otimes(1\ \ 1\ \ \cdots\ \ 1),$$

где (1 1 ... 1) – вектор с *n* единицами, *E* - единичная матрица порядка *m*.

Термин “*редуцированный*” в названии графа *G(n,m)* связан с тем, что при $mn\le n^t-1$ матрица $A(G(n,m))$ получается из матрицы смежности графа де Брейна степени *t* путем вычеркивания столбцов с номерами $\{nm+1,\ nm+2,\ \dots,\ n^t-1\}$ и строк с номерами $\{m,\ m+1,\dots,n^{t-1}-1,\ n^{t-1}+m,\ n^{t-1}+m+1,\dots,n^{t-1}+n^{t-1}-1,\ n^t+n^{t-1}+m,\dots,n^t-1\}$

Граф $G(n,n^{t-1})$ – это “обычный” граф де Брейна степени *t*, а граф $G\left(n^k,n^{t-k-1}\right)$ является его *k*-й степенью, т.е. графом переходов регистра сдвига с накопителем размера *t*, движущегося на k шагов за один такт.

Матрица $A(G(n,m))$ является n-циркулянтной. Поэтому в следующем разделе мы рассмотрим вопрос о спектре таких матриц.

Спектры k-циркулянтных матриц

Комплексная квадратная матрица $A=(a_{ij})_0^{N-1}$ порядка *N* называется *k* -циркулянтной, если каждая следующая ее строка получена из предыдущей циклическим сдвигом вправо на позиций.

Задача нахождения характеристического многочлена в случае *k=1* (обычный циркулянт) решается достаточно просто (см., например, [23]).

В работе [24] предложен способ нахождения спектра и собственных векторов *k*-циркулянтных матриц путем последовательных упрощений исходной матрицы преобразованиями подобия. Похожий метод, основанный на сведении задачи к отысканию спектра блочной матрицы (для конкретных классов *k*-циркулянтов), разработан в [25].

Основныь результатом данного раздела является выражение для характеристического многочлена произвольной k-циркулянтной матрицы в терминах элементов ее первой строки. Отметим, что в статье [26] получен аналогичный результат, но используется другое доказательство.

Теорема 1. Пусть комплексная квадратная матрица $A=(a_{ij})_0^{N-1}$ является *k*-циркулянтной порядка *N*, целые *N* и *k* представлены в виде разложения на простые множители: $k=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_d^{\alpha_d}$, $N=p_1^{\beta_1}p_2^{\beta_2}\dots p_d^{\beta_d}p_{d+1}^{\beta_{d+1}}\dots p_s^{\beta_s}$, где p_1, p_2 ... p_s – различные простые числа, $\alpha_i>0,\beta_j\ge 0$, $s\ge d$. Обозначим $\langle N,k\rangle=p_{d+1}^{\beta_{d+1}}\cdots p_s^{\beta_s}$, *w* и ε – примитивные корни из единицы степеней N и $\langle N,k\rangle$ соответственно, $\Omega_t=\{0,1,\dots,t-1\}$, $t=1,2,\dots$.

Тогда характеристический многочлен матрицы представим в виде:

$$\chi_A(\lambda)=\lambda^{N-\langle N,k\rangle}\prod_{c\in Cycles(\pi)}\left(\lambda^{l(c)}-\prod_{j\in c}\sum_{t=0}^{\langle N,k\rangle-1}\varepsilon^{tj}\sum_{s=0}^{\frac{N}{\langle N,k\rangle}-1}a_{s\langle N,k\rangle+t}\right),$$

где первое произведение берется по всем циклам с подстановки π, $\pi:i\to ki(\operatorname{mod}\langle N,k\rangle)$, $i\in\Omega_{\langle N,k\rangle}$, а второе – по всем числам *j*, образующим цикл *c*, *l(c)* - длина цикла *c*.

Доказательство. Обозначим $F=(w^{ij})_{i,j=0}^{N-1}$. Заметим, что $F^{-1}=\frac{1}{N}(w^{-ij})_{i,j=0}^{N-1}$.

Обозначим $B=(b_{ij})_{i,j=0}^{N-1}=F^{-1}AF$. Для элемента b_{ij} имеем:

$$b_{ij}=\frac{1}{N}\left\{\sum_{t=0}^{N-1}(w^{-1})^{it}\left(\sum_{l=0}^{N-1}a_{N-kt+l}w^{lj}\right)\right\},$$

где индексы у a_i берутся по модулю *N*. Поэтому:

$$b_{ij}=\frac{1}{N}\sum_{t,l}^{N-1}a_{N-kt+l}w^{lj-it}=\frac{1}{N}\sum_{p=0}^{N-1}a_p\sum_{t=0}^{N-1}w^{j(p-kt)-it}=\frac{1}{N}\sum_{p=0}^{N-1}a_pw^{jp}\sum_{t=0}^{N-1}w^{t(t-kj)}=$$

$$=\begin{cases}\sum_{p=0}^{N-1}a_pw^{jp}, & i=kj(\operatorname{mod}N)\\ 0, & i\ne kj(\operatorname{mod}N)\end{cases}$$

Очевидно равенство $\chi_A(\lambda)=\chi_B(\lambda)$.

Через ρ обозначим линейное отображение $\rho:i\to ki(\operatorname{mod}N),i\in\Omega_N$.

Пусть *G* – орграф отображения ρ на множестве вершин Ω_N. Каждая компонента связности этого графа является “пауком”, т.е. состоит из единственного цикла и подходов к нему.

Ненулевому элементу b_{ij} матрицы *B* соответствует дуга *(i, j)* в графе *G*. Перенумеруем элементы множества Ω_N в порядке перечисления компонент связности графа *G*. Тогда матрица *B* примет распавшийся вид:

$$B=\begin{pmatrix}B_0 & & & 0\\ & B_1 & & \\ & & \ddots & \\ 0 & & & B_L\end{pmatrix},$$

где блоки B_1 отвечают компонентам связности графа. Очевидно, $\chi_B(\lambda)=\prod_i\chi_{B_i}(\lambda)$.

Рассмотрим структуру блока B_j. В соответствующей компоненте связности графа *G* выделим цикл *c*. Пусть *l* - его длина, *T* - объем компоненты. *s* - одна из циклических вершин, $s\in\Omega_N$. Тогда $\rho^j(s)\ne s,\ j=1,2,\dots,l-1;\ \rho^l(s)=s$.

Выберем такую нумерацию, чтобы блок b_i принял полураспавшийся вид:

$$\left(\begin{array}{ccccc|ccc}0 & b_{\rho^{l-1}(s)\rho^{l-2}(s)} & 0 & \cdots & 0 & * & \cdots & *\\ 0 & \cdots & b_{\rho^{l-2}(s)\rho^{l-3}(s)} & \cdots & 0 & * & \cdots & *\\ \cdots & \cdots & \cdots & \ddots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots & b_{\rho(s)s} & * & \cdots & *\\ b_{s\rho^{l-1}(s)} & 0 & 0 & \cdots & 0 & * & \cdots & *\\ \hline 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0\\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0\end{array}\right).$$

Имеем

$$\chi_{B_i}(\lambda)=\lambda^{T-l}\left(\lambda^l-\prod_{s\in c}b_{\rho(s)s}\right) \tag{1}$$

Тогда $\chi_B(\lambda)=\lambda^{N-D}\prod_{c\in Cycles(\rho)}\left(\lambda^{l(c)}-\prod_{s\in c}b_{\rho(s)s}\right)$, где первое произведение берется по всем циклам ρ, второе - по всем точкам Ω_N, через которые проходит цикл *c*, *l(c)* - длина цикла *c*, *D* - общее количество циклических точек отображения ρ.

Кольцо вычетов Z_n представимо в виде прямой суммы идеалов (см. [27]) $Z_N=R_1\otimes\dots\otimes R_s$, где $R_i\cong Z_{p_i^{\beta_i}}$, i=1,2,...s, *i=1,2,...s*.

Рассмотрим ограничение ρ_i отображения ρ на идеал R_i. Если ρ_i/k, то отображение ρ_i нильпотентно, т.е.

$\rho_i^{\beta i}$ переводит все элементы идеала R_i в нуль. В противном случае, очевидно, отображение ρ_i является подстановкой. Граф отображения ρ является прямой суммой графов отображений ρ_i, i=1,2,…s. Пользуясь этим, установим взаимно-однозначное соответствие между циклами отображения ρ на множестве Ω_N и циклами подстановки π на множестве $\Omega_{\langle N,k\rangle}$. При этом циклу $c=\{s_1,s_2,\ldots,s_l \mid s_{i+1}=s_i\cdot k \bmod N,\ s_i\in\Omega_N\}$ отображения ρ соответствует цикл

$\bar{c}=\left\{\bar{s}_1=s_1\frac{\langle N,k\rangle}{N},\ldots,\bar{s}_l=s_l\frac{\langle N,k\rangle}{N}\right\}$ подстановки π,

а циклу $c'=\{s'_1,s'_2,\ldots,s'_l \mid s'_{i+1}=s'_i\cdot k \bmod\langle N,k\rangle,\ s'_i\in\Omega_{\langle N,k\rangle}\}$ подстановки π

соответствует цикл $\tilde{c}=\left\{\tilde{s}_1=s'_1\frac{N}{\langle N,k\rangle},\ldots,\tilde{s}_l=s'_l\frac{N}{\langle N,k\rangle}\right\}$ отображения ρ.

Возвращаясь теперь в (1) к произведению по точкам цикла с отображения ρ, имеем:

$$\prod_{s\in C} b_{\rho(s)s}=\prod_{s\in C} b_{sk(\bmod N)s}=\prod_{s\in C}\sum_p a_p w^{sp}=\prod_{\bar{s}\in\bar{c}}\sum_p a_p w^{\bar{s}p\frac{N}{\langle N,k\rangle}} \; c =\prod_{j\in c}\sum_{i=0}^{N-1} a_i\varepsilon^{ij},$$

где последнее произведение берется по соответствующему с циклу $\bar{c}$ подстановки π. Очевидно равенство:

$$\prod_{j\in \bar{c}}\sum_{i=0}^{N-1} a_i\varepsilon^{ij}=\prod_{j\in c}\sum_{t=0}^{\langle N,k\rangle-1}\varepsilon^{tj}\sum_{s=0}^{\frac{N}{\langle N,k\rangle}-1} a_{s\langle N,k\rangle+t}.$$

Число D циклических точек отображения ρ, очевидно, равно $\langle N,k\rangle$.

Теорема доказана. ■

Замечание 1. Если $k=1$, то для «обычного» циркулянта имеем $\chi_A(\lambda)=\prod_{j=0}^{N-1}\left(\lambda-\sum_{t=0}^{N-1}\varepsilon^{tj}a_t\right)$, что является хорошо известным фактом (см. [23]).

Замечание 2. Пусть s является степенью k. Тогда $\langle N,k\rangle=1$, подстановка π есть $\binom{0}{0}$, и по теореме 1 имеем

$$\chi_A(\lambda)=\lambda^{N-1}\left(\lambda-\sum_{t=0}^{N-1}a_t\right).$$

Последний результат позволяет выписать характеристический многочлен графа де Брейна, впервые полученный в [28].

Свойства редуцированного графа де Брейна.

Утверждение 2.

1. Число вершин в $G(n,m)$ равно nm, число ребер равно n^2m.

2. $G(n,m)$ – сильносвязный регулярный мультиграф степени n.

3. Для $G(n,m)$ реберным является граф $G(n,nm)$.

4. Диаметр графа G(n,m) равен $]\log_n nm[$, где $]x[$ – минимальное целое, не меньшее x.

Доказательство. п. 3. Пронумеруем дуги графа $G(n,m)$, перечисляя единицы его матрицы смежности в лексикографическом порядке: k-ая дуга выходит из вершины с номером $\left[\frac{k}{n}\right]$, и заходит в вершину с номером $k(\bmod\ nm)$, $k=0, 1,\ldots, n^2m-1$.

Граф, реберный к $G(n,m)$, содержит n^2m вершин. По определению реберного графа, i-ая и j-ая вершины соединены дугой тогда и только тогда, когда в графе $G(n,m)$ i-ая дуга заходит в такую вершину, из которой выходит j-ая дуга. Это условие равносильно равенству $i(\bmod nm)=\left[\frac{j}{n}\right]$, которое, очевидно, задает отношение смежности вершин в графе $G(n,nm)$.

п. 4. Выходящие из вершины $i\in\Omega_{nm}$ дуги заходят в вершины вида $(in+\varepsilon)(\bmod nm)$, $\varepsilon\in\Omega_n$. Поэтому семейство вершин, в которые существуют пути длины l из вершины i, имеет вид $\left\{in^l+\sum_{s=1}^{l}\varepsilon_s n^{l-1}(\bmod nm),\ \varepsilon_s\in\Omega_n,\ s=1,2,\ldots,l\right\}$.

Отсюда следует, что имеется не менее $\left[\frac{n^l}{nm}\right]$ и не боле $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, $m=p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k}p_{k+1}^{\beta_{k+1}}\ldots p_s^{\beta_s}$, е $\left[\frac{n^l}{nm}\right]+1$, путей длины l из вершины i в произвольную вершину j графа $G(n,m)$. В частности, диаметр графа $G(n,m)$ равен $]\log_n nm[$.■

Рассмотрим вопрос о спектрах редуцированных графов де Брейна.

Пусть n и m имеют следующие разложения на простые множители: $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, $m=p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k}p_{k+1}^{\beta_{k+1}}\ldots p_s^{\beta_s}$, где $p_1, p_2, \ldots, p_s$ – различные простые числа, $\alpha_i>0, \beta_j\ge 0$. $\langle n,m\rangle=p_{k+1}^{\beta_{k+1}}\ldots p_s^{\beta_s}$.

Теорема 3. Характеристический многочлен графа $G(n,m)$ имеет вид:

$$\chi(\lambda)=\lambda^{nm-\langle n,m\rangle}(\lambda-n)\prod_{k=1}^{\langle n,m\rangle-1}\left(\lambda^k-1\right)^{l_k}.$$

где l_k - количество циклов длины k в подстановке $\begin{pmatrix} i \\ ni(\bmod\langle n,m\rangle)\end{pmatrix}, i\neq 0$.

Доказательство. Матрица смежнсcти $A(G(n,m))$ графа $G(n,m)$ с является n-циркулянтом, поэтому данная теорема следует из теоремы 1. ■

Следствие. Для характеристических многочленов графов $G(n,mc$ и $G(n,nm)$ имеет место равенство:

$$\chi_{G(n,m)}(\lambda)=\lambda^{(n-1)nm}\chi_{G(n,nm)}(\lambda).$$

Таким образом, при переходе от графа $G(n,m)$ к его реберному графу $G(n,m)$ не появляется новых ненулевых значений в спектре графов, и также не меняется их кратность.

Рассмотрим количество контуров длин 1 и 2 в графе $G(n,m)$. В обычном графе де Брейна петли и контура длины 2 описываются следующим образом:

петли расположены при вершинах вида $(i\ i \ldots i)$, $i,j\in\Omega_n$, их ровно n;

контура длины 2 соединяют пары вершин $(i\ j\ i\ j \ldots)$ и $(j\ i\ j\ i \ldots)$, $i,j\in\Omega_n$, их ровно $\binom{n}{2}$.

Утверждение 4. В графе $G(n,m)$:

а) количество петель равно $n+(n-1, m)-1$.

б) количество контуров длины 2 равно $\binom{n}{2}+\frac{1}{2}\left((m,n^2-1)-(m,n-1)\right)$.

Доказательство. Пусть $\chi(\lambda)=\sum_{i=0}^{nm-1}a_i\lambda^i$ – характеристический многочлен графа $G(n,m)$, $A(G(n,m))$ – его матрица смежности. Число петель в графе равно следу матрицы смежности:

$$c_1=Tr(A(G(n,m)))=-a_{nm-1}. \tag{2}$$

Число c_2 контуров длины 2 в этом графе. Покажем, что имеет место равенство $c_2=\frac{Tr\left(A^2(G(n,m))\right)-Tr\left(A(G(n,m))\right)}{2}$. Действительно, диагональный элемент $a_{i,i}^{(2)}$ квадрата матрицы смежности равен количеству всех маршрутов длины два в графе, начальной и конечной точкой которых является вершина i. Промежуточной точкой такого маршрута является некоторая вершина в графе. Если эта вершина совпадает с i, то маршрут состоит из двукратного «путешествия» по петле, и общее число таких маршрутов выражается числом петель, т.е. $Tr\left(A^2\right)=-2a_{nm-2}+a_{nm-1}^2$. Если промежуточной точкой такого маршрута является вершина $j\neq i$, то маршрут является простым контуром длины два в графе. Поскольку простой контур проходит через пару вершин, то мы приходим к соотношени ю $Tr\left(A^2(G(n,m))\right)=Tr\left(A(G(n,m))\right)+2c_2$, эквивалентному доказываемой формуле. Заметим, что след матрицы есть сумма ее собственных чисел, а след квадрата матрицы есть сумма квадратов ее собственных чисел. Воспользовавшись соотношениями Ньютона ([29], с. 93) между коэффициентами характеристического многочлена матрицы и суммами его корней, несложно установить, что $Tr\left(A^2\right)=-2a_{nm-2}+a_{nm-1}^2$. Поэтому

$$c_2=\frac{a_{nm-1}^2-2a_{nm-2}+a_{nm-1}}{2}. \tag{3}$$

Обозначим $\vartheta(\lambda)=\lambda^{nm}\chi\left(\frac{1}{\lambda}\right)$. Тогда

$$a_{nm-1}=\frac{d}{d\lambda}\vartheta(\lambda)\Big|_{\lambda=0},\ a_{nm-2}=\frac{d^2}{d\lambda^2}\vartheta(\lambda)\Big|_{\lambda=0}. \tag{4}$$

Имеем: $\vartheta(\lambda)=\frac{\lambda^{nm}}{\lambda^{nm-\langle n,m\rangle}}\left(\frac{1}{\lambda}-n\right)\prod_{k=1}^{\langle n,m\rangle-1}\left(\frac{1}{\lambda^k}-1\right)^{l_k}=(1-n\lambda)\prod_{k=1}^{\langle n,m\rangle-1}\left(1-\lambda^k\right)^{l_k}$.

Стандартным путем вычислим первую производную:

$$\frac{d}{d\lambda}\vartheta(\lambda)=-n\prod_{k=1}^{\langle n,m\rangle-1}\left(1-\lambda^k\right)^{l_k}+(1-n\lambda)\sum_{k=1}^{\langle n,m\rangle-1}l_k\left(1-\lambda^k\right)^{l_k-1}\left(-k\lambda^{k-1}\right)\prod_{j\neq k}\left(1-\lambda^k\right)^{l_j}.$$

$$\begin{gathered}
\frac{d^2}{d\lambda^2}\vartheta(\lambda)=-n\sum_{k=1}^{\langle n,m\rangle-1}l_k\left(1-\lambda^k\right)^{l_k-1}\left(-k\lambda^{k-1}\right)\prod_{j\neq k}\left(1-\lambda^j\right)^{l_j}+\\
-n\sum_{k=1}^{\langle n,m\rangle-1}l_k\left(1-\lambda^k\right)^{l_k-1}\left(-k\lambda^{k-1}\right)\prod_{j\neq k}\left(1-\lambda^j\right)^{l_j}+\\
(1-n\lambda)\sum_{k=1}^{\langle n,m\rangle-1}\left\{\sum_{j\neq k}\left(-j\lambda^{j-1}\right)l_j\left(1-\lambda^j\right)^{l_j-1}\left(-k\lambda^{k-1}\right)l_k\left(1-\lambda^k\right)^{l_k-1}\prod_{i\neq j,k}\left(1-\lambda^i\right)^{l_i}+\right.\\
\left.\left(l_k(l_k-1)\left(1-\lambda^k\right)^{l_k-2}\left(-k\lambda^{k-1}\right)^2+l_k\left(1-\lambda^k\right)^{l_k-1}\left(-k(k-1)\lambda^{k-2}\right)\right)\prod_{j\neq k}\left(1-\lambda^j\right)^{l_j}\right\}=\\
-2n\sum_{k=1}^{\langle n,m\rangle-1}l_k\left(1-\lambda^k\right)^{l_k-1}\left(-k\lambda^{k-1}\right)\prod_{j\neq k}\left(1-\lambda^j\right)^{l_j}+\\
(1-n\lambda)\sum_{k=1}^{\langle n,m\rangle-1}\left\{\sum_{j\neq k}jkl_jl_k\lambda^{j+k-2}\left(1-\lambda^j\right)^{l_j-1}\left(1-\lambda^k\right)^{l_k-1}\prod_{i\neq j,k}\left(1-\lambda^i\right)^{l_i}+\right.\\
\left.\left(l_k(l_k-1)\left(1-\lambda^k\right)^{l_k-2}\left(-k\lambda^{k-1}\right)^2+l_k\left(1-\lambda^k\right)^{l_k-1}\left(-k(k-1)\lambda^{k-2}\right)\right)\prod_{j\neq k}\left(1-\lambda^j\right)^{l_j}\right\}.
\end{gathered}$$

Подставляя в полученные выражения $\lambda=0$, имеем:

$$\frac{d}{d\lambda}\vartheta(\lambda)\Big|_{\lambda=0}=-(n+l_1) \tag{5}$$

$$\frac{d^2}{d\lambda^2}\vartheta(\lambda)\Big|_{\lambda=0}=2nl_1+l_1(l_1-1)-2l_2. \tag{6}$$

Вычислим l_1 и l_2.

Согласно определению. l_1 равно числу ненулевых решений сравнения $i=ni\ (\mathrm{mod}\langle n,m\rangle)$, или $i(n-1)=0\ (\mathrm{mod}\langle n,m\rangle)$. Поэтому $l_1=(n-1\langle N,m\rangle)-1$. Но $(n,n-1)=1$, следовательно, $l_1=(n-1,m)-1$. (7)

Объединяя (2), (3, (4) и (7), заключаем, что число петель в графе $G(n,m)$ равно n+ $(n-1,m)-1$.

Величина l_2 определяется как количество циклов длины 2 в подстановке $\begin{pmatrix} i \\ ni(\mathrm{mod}\langle n,m\rangle)\end{pmatrix}$, т.е. как половина числа решений системы

$$\begin{cases} i=n^2i\left(\mathrm{mod}\langle n,m\rangle\right),\\ in\neq i\left(\mathrm{mod}\langle n,m\rangle\right).\end{cases}$$

Число решений первого сравнения равно (n^2-1,m). Число решений сравнения $in=i(\mathrm{mod}\langle n,m\rangle)$, или $i(n-1)=0(\mathrm{mod}\langle n,m\rangle)$, равно $(n-1,m)$, причем каждое его решение одновременно является решением первого сравнения. Следовательно, рассматриваемая система имеет в точности $(n^2-1,m)-(n-1,m)$ решений и поэтому

$$l_2=\frac{\left(n^2-1,m\right)-\left(n-1,m\right)}{2}. \tag{8}$$

Объединяя (3), (4), (5) и (8), заключаем, что число контуров длины 2 в графе $G(n,m)$ равно $\binom{n}{2}+\frac{1}{2}\left(\left(m,n^2-1\right)-\left(m,n-1\right)\right)$.■

Орграф G обладает свойством *единственности пути длины t* ([16], [17]), если между любыми двумя его вершинами существует ровно один путь длины t. Граф де Брейна степени t обладает таким свойством, поскольку из вершины $(\alpha_1, \alpha_2, \dots, \alpha_t)$ в вершину $(\beta_1, \beta_2, \dots, \beta_t)$ за t шагов можно перейти единственным способом. Следующее утверждение показывает уникальность этого свойства в семействе редуцированных графов де Брейна.

Утверждение 5. Граф $G(n,m)$ обладает свойством единственности пути длины t тогда и только тогда, когда $m=n^{t-1}$.

Доказательство. Достаточность рассматриваемого условия очевидна.

Докажем необходимость. Пусть J - квадратная матрица порядка nm, состоящая из единиц. Если для некоторого натурального t граф $G(n,m)$ обладает свойством единственности пути длины t, то $(A(G(n,m))t=J$.

Из теоремы 3 следует, что $\lambda_1=n$, – максимальное собственное число графа G(n,m). Приравнивая максимальные собственные значения матриц в предыдущем равенстве, получаем $n^t=nm$. ■

Число остовных деревьев и эйлеровых циклов редуцированного графа де Брейна устанавливает

Утверждение 6. Число $T(G(n,m))$ остовных деревьев графа $G(n,m)$ равно

$$T\left(G(n,m)\right)=\frac{1}{nm}n^{nm-\langle n,m\rangle}\prod_{k=1}^{\langle n,m\rangle-1}\left(n^k-1\right)^{l_k},$$

число $C(G(n,m))$ эйлеровых циклов в графе $G(n,m)$ равно

$$C\left(G(n,m)\right)=\left((n-1)!\right)^{nm}\frac{n^{nm-\rangle n,m\langle}}{nm}\prod_{k=1}^{\rangle n,m\langle-1}\left(n^k-1\right)^{l_k},$$

где l_k - количество циклов длины k в подстановке $\begin{pmatrix} i \\ ni\left(\mathrm{mod}\langle n,m\rangle\right)\end{pmatrix},\ i\neq 0$.

Доказательство. Воспользуемся результатом Хученройтера [30], который состоит в следующем. Пусть G – регулярный мультиграф степени n на N вершинах, с собственными значениями $\lambda_1=n$, λ_2, …, λ_N. Тогда для числа $T(G)$ остовных деревьев графа G справедливо соотношение

$$T(G)=\frac{1}{N}\prod_{i=2}^{N}(n-\lambda_i).$$

Для графа согласно теореме 3 имеем

$$T(G(n,m))=\frac{1}{nm}n^{nm-\langle n,m\rangle}\prod_{k=1}^{\langle n,m\rangle-1}\prod_{j=1}^{l_k}\prod_{i=1}^{k}\left(n-w_k^i\right),$$

где w_k – примитивный корень k-й степени из единицы.

Для доказательства первого пункта утверждения достаточно убедиться, что $\prod_{i=1}^{k}\left(n-w_k^i\right)=n^k-1$. Рассмотрим выражение $f(x)=\prod_{i=1}^{k}\left(x-w_k^i\right)$, где x – формальная переменная. Очевидно, $f(x)$ – многочлен от x степени k. Его корнями являются все различные корни из единицы. С другой стороны, у многочлена x^k-1 в точности то же множество корней. Поэтому $f(x)=x^k-1$.

Доказательство второго пункта утверждения состоит в подстановке найденного выражения для $T(G(n,m))$ в формулу

$$C(G)=T(G)\prod_{i=1}^{N}(d_i-1)!$$

для числа $C(G)$ эйлеровых циклов в эйлеровом орграфе G порядка N, где d_i - степень захода вершины i, $i=1, 2,\ldots,N$.■

Результат теоремы 3 позволяет предложить новое и сравнительно (см. [1] и [28]) простое доказательство классической формулы Гуда - де Брейна о числе полноцикловых регистров сдвига.

Утверждение 7. Количество n-ичных полноцикловых регистров сдвига с накопителем длины t равно

$$\frac{(n!)^{n^{t-1}}}{n^t}.$$

Доказательство. В случае “обычного” графа де Брейна на nt вершинах имеем $m=n^{t-1}$, $\langle n,m\rangle=1$, поэтому характеристический многочлен матрицы смежности этого графа по теореме 3 равен $\chi_{G_t}(\lambda)=\lambda^{k^t-1}(\lambda-k)$.

Все собственные числа графа равны нулю, за исключением $\lambda_1=n$, , и согласно полученным выше формулам

$$T(G_t)=T\left(G\left(n,n^{t-1}\right)\right)=\frac{n^{n^t-1}}{n^t}=n^{n^t-t-1},$$

$$C(G_t)=C\left(G\left(n,n^{t-1}\right)\right)=\frac{(n!)^{n^t}}{n^{t+1}}.$$

Для доказательства утверждения осталось заметить, что количество k-ичных полноцикловых регистров сдвига с накопителем длины t совпадает с числом эйлеровых циклов в D_{t-1}.■

Замечание 3. «Экстремальным» случаем значений параметров m и n является случай, когда n - примитивный корень по модулю m, т. е. когда множество $\left\{n^j(\mathrm{mod}\, m),\ j=1,2,\ldots,m-1\right\}$ совпадает с множеством всех ненулевых вычетов по модулю m. В этом случае $\langle n,m\rangle=m$. По утверждению 6 имеем

$$T(G(n,m))=\frac{n^{(n-1)m}}{nm}\left(n^{m-1}-1\right)=n^{nm}\left(\frac{1}{mn^2}-\frac{1}{mn^{m+1}}\right),$$

$$C\left(G\left(n,n^k\right)\right)=\left((n-1)!\right)^{nm}n^{nm}\left(\frac{1}{n^2m}-\frac{1}{mn^{m+1}}\right)=(n!)^{nm}\left(\frac{1}{mn^2}-\frac{1}{mn^{m+1}}\right).$$

Замечание 4. Поскольку граф *G(n,m)* является реберным для графа *G(n,m)*, то множество эйлеровых циклов в графе *G(n,m)* совпадает с множеством гамильтоновых циклов в *G(n,m)*.

Выводы

Изучены характеристики подкласса обобщенных в смысле Imase и Ito графов де Брейна, названных редуцированными графами де Брейна. Получен вид характеристического многочлена матрицы смежности таких графов. Спектральными методами для этих графов вычислены число петель и циклов длины 2, а также число остовных деревьев и эйлеровых циклов. Для редуцированных графов де Брейна вычислены диаметры и описано множество значений параметров, при которых графы обладают свойством единственности пути заданной длины. Для получения этих результатов разработан новый способ вычисления характеристического многочлена k-циркулянтной матрицы в терминах элементов ее первой строки.

Это позволило также уточнить и упростить доказательство ряда известных результатов о графах де Брейна и предложить более простые процедуры вычисления характеристического многочлена указанных матриц.

В отношении использования архитектуры редуцированных графов де Брейна в целях контроля защищенности информационных систем с составным числом элементов и управления подсистемами защиты элементовтаких систем следует отметить ряд свойств этих графов, установленнных в даннной статье:

- малый диаметр графа позволяет быстро получать сведения об изменении состояния элемента системы (утверждение 2);

- имеются условий для реализации масштабируемых подсистем контроля и управления за счет использовния дуальности редуцированного графа де Брейна и его реберного графа (утверждение 2)

- существует возможность выбора таких настроек системы контроля, чтобы снизить вероятность зацикливния при обходе вершин графа (элементов системы) за счет малости числа петель и циклов длины 2 (утверждение 4);

- возможно гибко перестраивать маршруты обхода всех элементов системы благодаря значительному числу эйлеровых циклов (утверждение 6);

__Рецензент:__ Калашников Андрей Олегович, доктор технических наук, заместитель директора ФГБУН Институт проблем управления им. В.А. Трапезникова РАН, г. Москва, Россия. E-mail: tigrilla1962@mail.ru

Литература

1 Холл М. Комбинаторика. - М.: Мир, 1970. – 424 с.

2. Golomb S.W. Shift Register Sequences. – Aegean Park Press. - Laguna Hills, Calif. - 1981. – 247 p.

3. Bermond J.C., Peyrat C. De Bruijn and Kautz Networks: A competitor for the Hypercube? // European Workshop on Hypercubes and Distributed Computers, pp. 279–293. Elsevier, 1989.
4. Hosseinabady M., Kakoee M.R., Mathew J., Pradhan D.K. De Bruijn graph as a low latency scalable architecture for energy efficient massive NoCs // Proc. Conf. on Design, automation and test in Europe, Munich, pp. 1370-1373, 2008.
5. Loguinov D., Kumar A., Rai V., Ganesh S. Graph-theoretic analysis of structured peer-to-peer systems: Routing distances and fault resilience // ACM SIGCOMM, pp. 395-406, 2003.
6. Compeau P., Pevzner P., Tesler G. How to apply de Bruijn graphs to genome assembly // Nature Biotechnology. – 2011. –V.29. –pp. 987–991.
7. Блейхут Р. Теория и практика кодов, контролирующих ошибки. М: Книга по требованию, 2013. 566 с.
8. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие — М.: Гелиос АРВ, 2002. — 480 с.
9. Шрейер Брюс Прикладная криптография. Протоколы, алгоритмы и тексты на языке С. – Вильямс, 2016. – 1024 с.
10. Imase M., Itoh M. Design to minimize diameter on building-block networks // IEEE Trans. Comput. 30 (1981), pp. 439–442.
11. Imase M., Itoh M. A design for directed graphs with minimum diameter // IEEE Trans. Comput. 32 (1983), pp. 782–784.
12. Reddy S.M., Pradham D.K., Kuhl J.G. Directed graphs with minimum diameter and maximal connectivity // Tech. Rep. School Eng. Rochester, Oakland Univ., 1980.
13. Du D. Z., Hwang F. K. Generalized de Bruijn digraphs // Networks 18 (1) (1988), pp. 27–38.
14. Xueliang Li, Fuji Zhang. On the numbers of spanning trees and Eulerian tours in generalized de Bruijn graphs, Discrete Math. 91 (1991) 189–197.
15. Ню В. О числе внешней устойчивости обобщенных графов де Брейна // Сиб. журн. исслед. операций, 1994, том 1, N2, С. 61-66.
16. Малышев Ф.М., Тараканов В.Е. Обобщенные графы де Брейна // Матем. заметки, 1997, т. 62, №4, С. 540-548.
17. Тараканов В.Е. О группах автоморфизмов обобщенных графов де Брейна // Труды по дискр. матем., 2002, т.5. С. 235-240.
18. Сачков В.Н., Тараканов В.Е. Комбинаторика неотрицательных матриц. М., изд-во ТВП, 2000, 448 с.
19. Yao-Kun Wu, Rui-Zhong Jia, Qiao Li. g-circulant solutions to the (0, 1) matrix equation . // Linear Algebra and Appl., 2002, Vol. 345, p. 195-224.
20. Максимовский А.Ю., Мельников С.Ю. О планарности одного подкласса обобщенных графов де Брейна // Обозрение прикладной и промышленной математики, 2011, т.18, вып.4, С. 647-648.
21. Максимовский А.Ю., Мельников С.Ю. О числе обобщенных в смысле Imase и Itoh регистров сдвига, устанавливаемых постоянным входом в фиксированное состояние. // Обозрение прикладной и промышленной математики. – 2015. – Т. 22. Вып. 5, С. 522.
22. Максимовский А.Ю. О групповых свойствах подстановок, определенных на смежных классах конечной абелевой группы составного порядка по ее подгруппам. Математические вопросы криптографии., 2016, Т.7, № 1, С. 83-92.
23. Маркус М., Минк Х. Обзор по теории матриц и матричных неравенств. М, Наука, 1972. - 232 с.
24. Ablow C.M., Brenner J.L. Roots and canonical forms for circulant matrices // Trans. Amer. Math. Soc. - 1963, v. 107, N2, pp. 360-376.
25. Строк В.В. Циркулянтные матрицы и спектры графов де Брейна // Укр. мат. журн., 1992, т.44, N 11, С. 1571-1579.
26. Zhou Jin-tu. The diagonalization condition for g-circulant matrix. (Кит., рез. англ.) // Zhejiang Norm. Univ. Natur. Sci., 2004, Vol. 27, N4, pp. 325-328.
27. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. - М. : Гелиос АРВ. - 2003. - Т.2. - 414с.
28. Строк В.В. Спектры графов некоторых классов последовательностей // - В кн.: Всесоюз. алгебраич. симпоз. Тез. докл. В 2-х ч. Гомель: Изд. АН СССР - АН БССР, 1975. - ч.2, С. 452.
29. Гантмахер Ф.Р. Теория матриц. -5-е изд., - М., ФИЗМАТЛИТ, 2004, -560 с.
30. Цветкович Д., Дуб М., Захс Х. Спектры графов. Теория и применение. // Киев: «Наукова думка», 1984. - 384 с.

SPECTRAL AND COMBINATORIAL CHARACTERISTICS OF THE REDUCED DE BRIJN GRAPHS

Maksimovskiy A.Yu.[3], Melnikov S.Yu.[4]

The spectral and combinatorial characteristics of a subclass of generalized de Bruijn digraphs are investigated. The spectra, diameters, number of loops and cycles of length 2, as well as the number of spanning trees, Eulerian and Ham-

3 Alexander Yu. Maksimovskiy, Ph.D. (Math.), Associate Professor, Institute for Management Problems V.A. Trapeznikova RAS, Moscow, Russia. E-mail: maximay@ipu.ru

4 Sergey Yu. Melnikov, Ph.D. (Math.), Associate Professor, Linguistic and Information Technologies, LLC, Moscow, Russia. E-mail: melnikov@linfotech.ru

iltonian cycles of such graphs are calculated. The considered class of digraphs is closed with respect to the operation of constructing the line digraph. The obtained values of these characteristics indicate the expediency of applying such graphs in the design of subsystems for monitoring the security of information systems with a composite number of elements. This is due to the fact that for control subsystems that use the architecture of a graph with established properties, it is possible to provide effective access to all elements of the system as a whole, its scalability, flexible configuration of routes to bypass elements with a minimum risk of looping. When studying the influence of the numerical parameters of the graphs under consideration on their properties, it was found that the uniqueness property of a path of a given length is preserved only for "ordinary" de Bruijn graphs. To obtain these results, a new method for calculating the characteristic polynomial of the k-circulant matrix in terms of the elements of its first row has been developed. This also made it possible to clarify a number of known results and simplify the procedures for calculating the characteristic polynomial of these matrices.

Key words: *shift register, k-circulant, de Bruijn graph, matrix spectrum*

References

1. Holl M. Комbinatoriка. - M.: Mir, 1970. – 424 p.
2. Golomb S.W. Shift Register Sequences. – Aegean Park Press. - Laguna Hills, Calif. - 1981. – 247 p
3. Bermond J.C., Peyrat C. De Bruijn and Kautz Networks: A competitor for the Hypercube? // European Workshop on Hypercubes and Distributed Computers, pp. 279–293. Elsevier, 1989.
4. Hosseinabady M., Kakoee M.R., Mathew J., Pradhan D.K. De Bruijn graph as a low latency scalable architecture for energy efficient massive NoCs // Proc. Conf. on Design, automation and test in Europe, Munich, PP. 1370-1373, 2008
5. Loguinov D., Kumar A., Rai V., Ganesh S. Graph-theoretic analysis of structured peer-to-peer systems: Routing distances and fault resilience // ACM SIGCOMM, pp. 395-406, 2003.
6. Compeau P., Pevzner P., Tesler G. How to apply de Bruijn graphs to genome assembly // Nature Biotechnology. – 2011. –V.29. –PP. 987–991.
7. Bleihut R. Teoriya и praktika kodov, kontroliruyuschih oshibki M: Kniga po trebovaniyu, 2013. 566 p.
8. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Osnovy kriptografii. Uchebnoe posobie — M.: Gelios ARV, 2002. — 480 p.
9. Shreier Bryus Prikladnaya kriptografiya. Protokoly, algoritmy i teksty na yazyke C. – Vilyams, 2016. – 1024 p.
10. Imase M., Itoh M. Design to minimize diameter on building-block networks // IEEE Trans. Comput. 30 (1981) 439–442.
11. Imase M., Itoh M. A design for directed graphs with minimum diameter // IEEE Trans. Comput. 32 (1983) 782–784.
12. Reddy S.M., Pradham D.K., Kuhl J.G. Directed graphs with minimum diameter and maximal connectivity // Tech. Rep. School Eng. Rochester, Oakland Univ., 1980.
13. Du D. Z., Hwang F. K. Generalized de Bruijn digraphs // Networks 18 (1) (1988), 27–38.
14. Xueliang Li, Fuji Zhang. On the numbers of spanning trees and Eulerian tours in generalized de Bruijn graphs, Discrete Math. 91 (1991) 189–197.
15. Nyu V. O chisle vneshnnei ustoichivosti obobschennyh grafov de Breina//Sib. zhurn. issled. operatsii, 1994, Vol 1, No2, pp.61-66.
16. Malyshev F.M., Tarakanov V.E. Obobschennye grafy de Breina //Matem. zmetki, 1997, V. 62, No4, pp. 540-548.
17. Tarakanov V.E. Ogruppah avtomorfizmov obobschennyh grafov de Breina // Trudy po diskr. matem., 2002, V.5. pp.235-240.
18. Sachkov V.N., Tarakanov V.E. Kombinatorika neotritsatelnyh matrits. M., TVP, 2000, 448 p.
19. Yao-Kun Wu, Rui-Zhong Jia, Qiao Li. g-circulant solutions to the (0, 1) matrix equation . // Linear Algebra and Appl., 2002, Vol. 345, p. 195-224.
20. Maksimovskiy A.Yu., Melnikov S.Yu. O planarnosti odnogo podklassa obobschennyh grafov de Breina // Obozrenie prikladnoi i promyshlennoy matematiki, V.18, dyp.4, pp. 647-648, 2011
21. Maksimovskiy A.Yu., Melnikov S.Yu. O chisle obobschnyh v smysle Imase и Itoh regitrov sdviga, ustnavlivaemyh postoyannym vhodom v fiksirovannoe sostoyanie . // Obozrenie prikladnoi i promyshlennoy matematiki, . – 2015. – Vol. 22. Vyp. 5.
22. Maksimovskiy A.Yu. O gruppovyh svoivvah podstnovok, opredelennyh na smezhnyh klassah konechnoi abelevoi grurry po ee podgruppam. Matematicheskie voprosy kriptografii, 2016, Vol.7, No 1, pp. 83-92.
23. Markus M., Mink H. Obzor po neorii matrits i mftrichnyh neravenstv. M, Nauka, 1972. - 232 p.
24. Ablow C.M., Brenner J.L. Roots and canonical forms for circulant matrices // Trans. Amer. Math. Soc. - 1963, v. 107, N2, pp. 360-376.
25. Strok V.V. Tsirkulyantnye matritsy I spektry grafov de Breina // Ukr. mat. zhurn., 1992, V.44, No 11, pp. 1571-1579.
26. Zhou Jin-tu. The diagonalization condition for g-circulant matrix. (Кит., рез. англ.) // Zhejiang Norm. Univ. Natur. Sci., 2004, Vol. 27, N4, p. 325-328.
27. Gluhov M. M., Elizarov V. P., Nechaev A. A. Algebra. - M. : Gelios ARV. - 2003. - Vol.2. – 414p.
28. Strok V.V. Spektry grafov nekotoryh klassov posledovatelnostei // - V kn.: Vsesoyuz. algebraich. simpoz. Tez. Dokl. V 2-h ch. Gomel: Izd. AN SSSR - AN BSSR, 1975. - ch.2, p.452.
29. Gantmaher F.R. Teoriya matrits. -5-e izd., - M., FIZMATLIT, 2004, -560 p.
30. Tsvetkovich D., Dub M., Zahs H. Spektry grafov. Teriya i primenenie. // Kiev: «Naukova dumka», 1984. - 384 p.